Claims

1. Method for providing connection security for the transmission between communicating parties in a telecommunication network, the method comprising the steps of:

exchanging security parameters between communicating parties,

providing connection security for messages based on these security parameters, and

transmitting said messages between communicating parties,

characterized in that the method further comprises the steps of:

reaching agreement between communicating parties on an interval for recalculation of the security parameters,

monitoring of the interval for recalculation by the communicating parties,

recalculating the security parameters at the agreed interval, and

providing connection security for messages based on the latest recalculated security parameters.

2. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the step of

ciphering messages based on the latest recalculated security parameters.

3. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the step of

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

4. Method according to claim 1, characterized in that providing connection security for messages based on the latest recalculated security parameters comprises the steps of

ciphering messages based on the latest recalculated security parameters, and

authenticating and providing integrity for the messages based on the latest recalculated security parameters.

5. Method according to claim 3 ~~or 4~~, characterized in that authenticating and providing integrity for the messages is arranged with a message authentication code MAC.

6. Method according to claim 1, characterized in that the method further comprises the steps of:

numbering the messages,

agreeing on the number of messages to determine the interval for the recalculation of the security parameters,

recalculating the security parameters after the agreed number of messages have been transmitted.

7. Method according to claim 6, characterized in that the method further comprises the steps of:

numbering the messages with sequence numbers,

transmitting the sequence number with the message, and

using the latest sequence number as input for recalculation of the security parameters.

8. Method according to claim 1, characterized in that the method comprises the step of

reaching agreement between communicating parties during hand-shaking on the interval for recalculation of the security parameters.